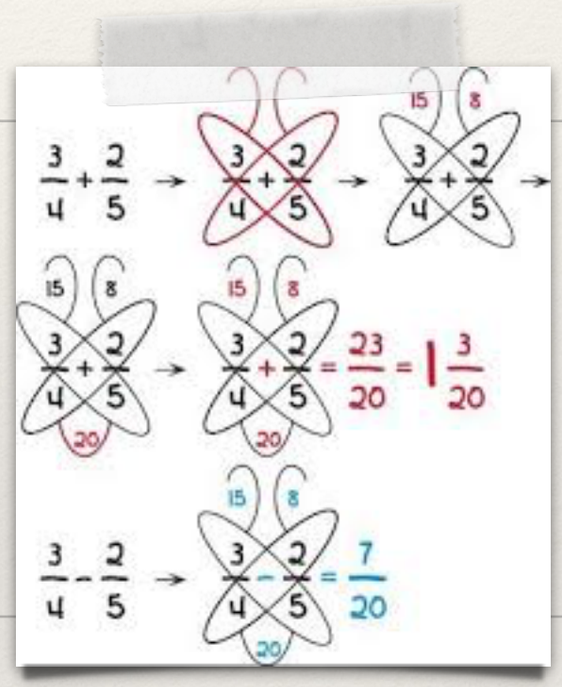


Partie 1:Maths discrètes

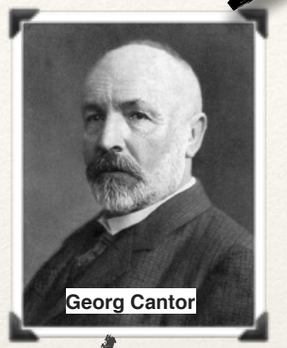
Session: Automne 2019
Professeur: Louis Salvail (salvailATiro.umontreal.ca)
bureau: A.-A. 3369

Langage dans lequel les mathématiques modernes so exprimées.

La logique est l'instrument qui fait progresses la science. (-384- -322)

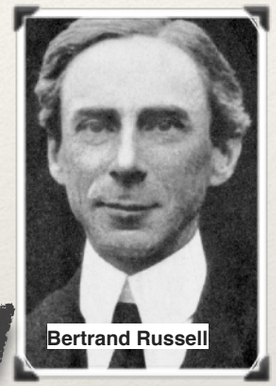
Créateur de la théorie des ensembles (1845-1918)

(Parti


Georg Cantor

1. Ensembles et logique
   - Ensembles (1.1)
   - Propositions (1.2-1.3)
   - Arguments et règles d'inférence (1.4)
   - Quantificateurs (1.5-1.6)

Logique des propositions


Bertrand Russell


Aristot

Logique*=Mathématiques (1872-1970)


Friedrich Ludwig Gottlob Frege

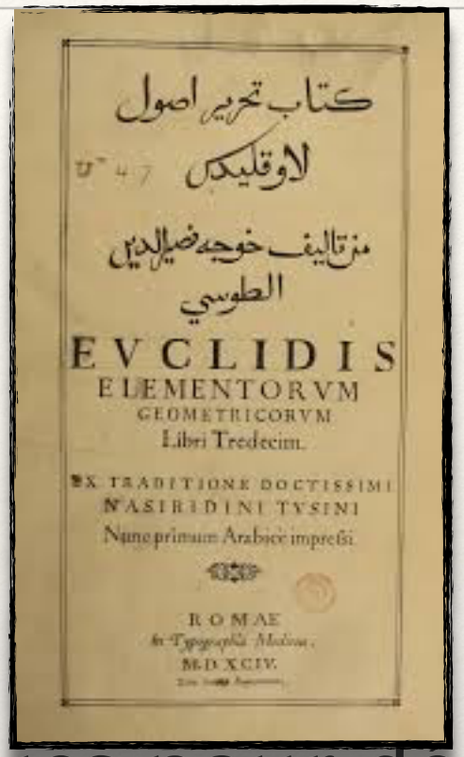
Logique des prédicats

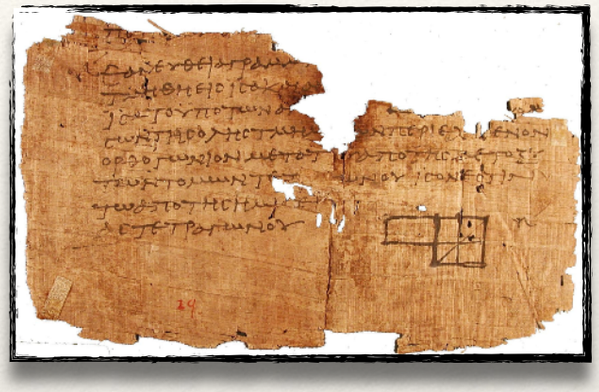
Mathématiques=Extension de la logique (1848-1925)

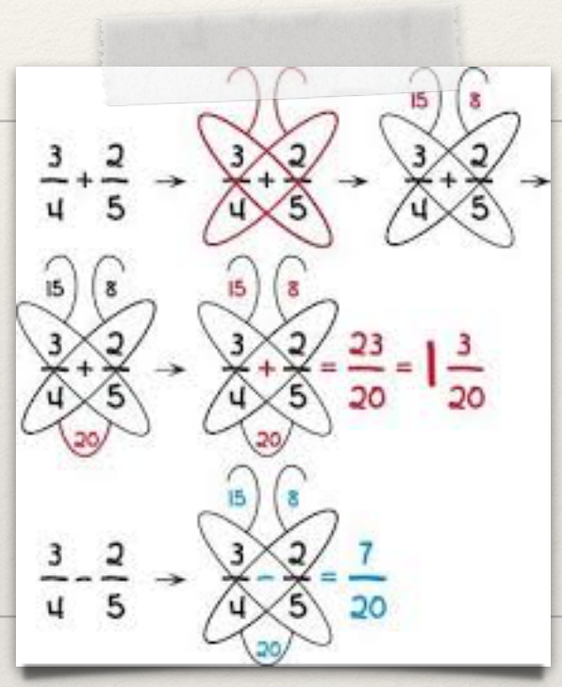
Table des matières (II)

2. Preuves

- Techniques de base (-2.3)
- Preuves par induction (2.4-2.5)
- Nous appliquerons ces techniques pour démontrer des propriétés importantes des entiers naturels.
- Les plus belles réalisations de l'informatique reposent en définitive sur ces propriétés importantes.





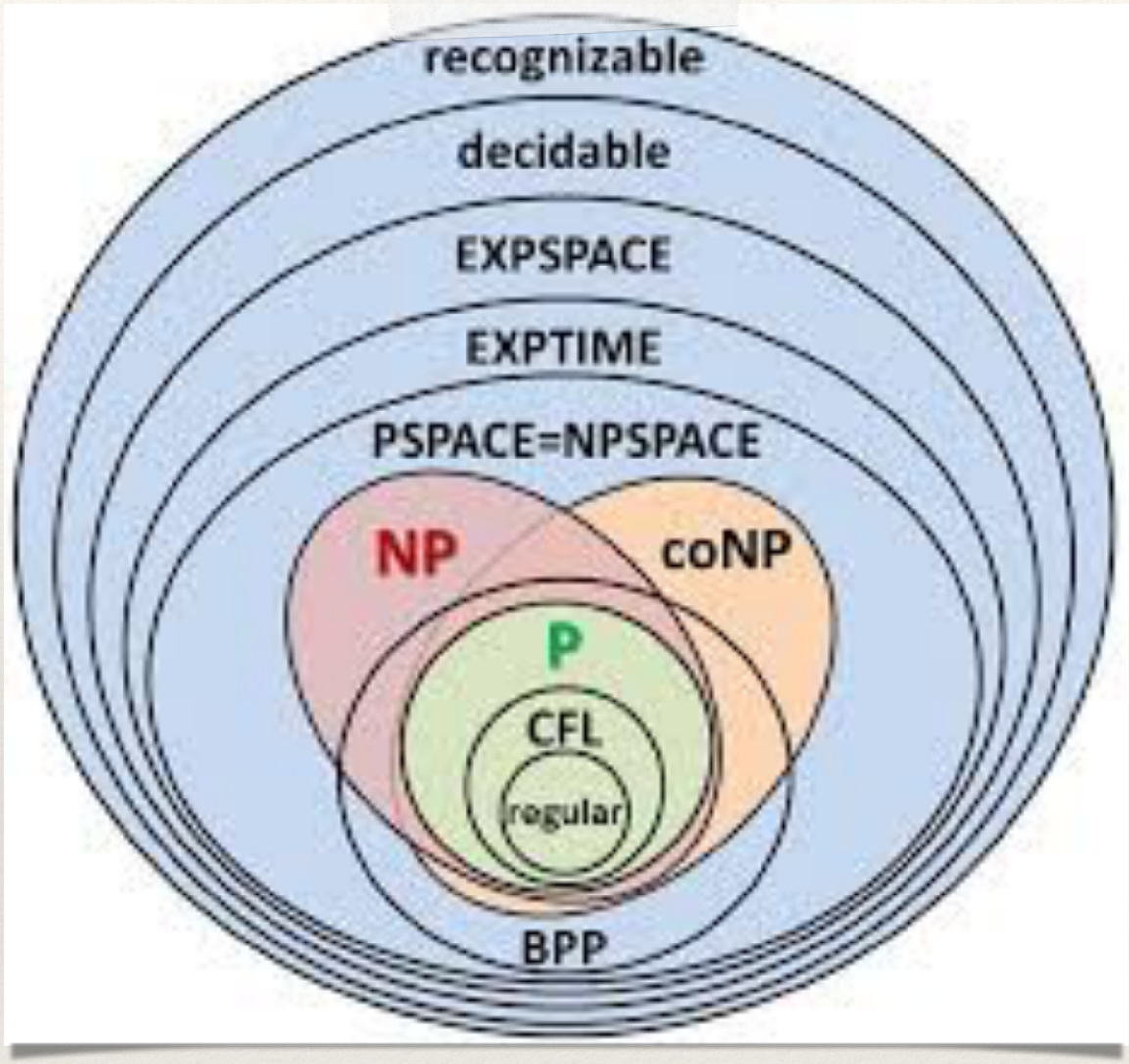


Partie 1:Maths discrètes

Session: Automne 2018
Professeur: Louis Salvail (salvailATiro.umontreal.ca)
bureau: A.-A. 3369

Chapitre 1 partie 1

Un peu de théorie des ensembles



Ensembles

- Objets mathématiques tellement généraux que les mathématiques peuvent être formulées dans leur langage.
- Les énoncés mathématiques sont la plupart du temps exprimés dans le langage de la théorie des ensembles.
- À la base, la théories des ensembles formalise les opérations naturelles que l'ont peut appliquer à des collection d'objets:
- **Défn:** Un *ensemble* est une collection d'objets. Les objets d'un ensemble sont appelés *éléments*.

Ensembles (II)

{...} désigne une ensemble.

- Un ensemble peut être donné par une équation du type:

$$A=\{patate, carotte, robinet\}$$

qui décrit un ensemble de 3 éléments: '*patate*', '*carotte*' et '*robinet*' que nous nommerons A.

- L'ordre dans lequel les éléments de A sont donnés n'est pas important:

$$A=\{carotte, robinet, patate\}=\{patate, robinet, carotte\}$$

Ensembles (III)

- Les ensemble ne sont définis que par les éléments distincts qu'ils contiennent:

$$A=\{patate, carotte, robinet\}$$

$$=\{patate, carotte, carotte, robinet\}$$

- Les éléments d'un ensemble peuvent être donnés par une propriété qu'ils doivent satisfaire:

tel que

$$P=\{x \mid x \text{ est un nombre premier}\}$$

- **Défn:** Un entier naturel est dit *premier* s'il est plus grand que 1 et n'est divisible sans reste que par 1 et lui-même.

- Un autre exemple:

$$C=\{x \mid x \text{ est une chaîne binaire de longueur finie qui débute par 1}\}$$

Ensemble (IV)

- Un ensemble peut évidemment contenir des ensembles comme éléments:

B={{*patate*, *carotte*}, {*carotte*, *robinet*}}

- L'ensemble B contient deux éléments, {*patate*, *carotte*} et {*carotte*, *robinet*}.

- B ne contient ni *patate*, ni *carotte*, ni *robinet* comme élément.

Des ensembles que nous connaissons

- **N**={0,1,2,3,4,...} est l'ensemble des entiers naturels.
- **N***={1,2,3,4,...} est l'ensemble des entiers naturels non-nuls.
- **Z**={...,-3,-2,-1,0,1,2,3,...} est l'ensemble des entiers.
- **Z***={...,-3,-2,-1,1,2,3,...} est l'ensemble des entiers non-nuls.
- **Q** est l'ensemble des entiers rationnels (de la forme a/b pour a un entier et b un entier naturel non-nul).
- **R** est l'ensemble des nombres réels.
- **C** est l'ensemble des nombres complexes (de la forme $a+b\cdot\sqrt{-1}$ pour a et b des nombres réels).

Cardinalité

- **Défn:** La *cardinalité (ou la taille)* d'un ensemble S, notée $|S|$, qui contient un nombre fini d'éléments est le nombre de ses éléments. Si S contient un nombre infini d'éléments alors nous dirons que la cardinalité de S est *infinie*, notée $|S|=\infty$.

- Nous avons $|\{\mathbf{N}\}|=|\{\mathbf{R}\}|=|\{\mathbf{Q}\}|=1$, mais $|\mathbf{N}|=|\mathbf{R}|=|\mathbf{Q}|=|\mathbf{C}|=\infty$.

- D'après vous,

$|P|=?$

La réponse à cette question a été donnée par Euclide vers -300.

- L'ensemble qui ne contient aucun élément, appelé *ensemble vide*, sera noté:

{} ou ∅

Appartenance

- Si x est un élément de l'ensemble S alors nous écrirons

$$x \in S$$

- Si x n'est pas un élément de S alors nous écrirons

$$x \notin S$$

- Nous pouvons maintenant définir l'ensemble des nombres rationnels de la façon suivante:

$$\mathbf{Q} = \{a/b \mid a \in \mathbf{Z} \text{ et } b \in \mathbf{N}^*\}$$

Égalité et inclusion

- **Défn:** Nous dirons de deux ensemble A et B qu'ils sont *égaux*, noté $A=B$, si

  1. chaque élément $x \in A$ est tel que $x \in B$ et
  2. chaque élément $x \in B$ est tel que $x \in A$.

  Si A et B sont des ensembles qui satisfont la condition 1. donnée plus haut alors nous dirons que A est un *sous-ensemble* de B, noté $A \subseteq B$.

- Nous avons donc que $A=B$ si et seulement si $A \subseteq B$ et $B \subseteq A$.

- **Défn:** Si $A \subseteq B$ et $A \neq B$ alors nous dirons que A *est un sous-ensemble strict de* B, noté $A \subset B$.

Égalité et inclusion (II)

- Est-ce que

$$\{x\in\mathbf{R} \mid x^2+2x+1=0\}=\{x\in\mathbf{Z} \mid x^2+2x+1=0\}=\{x\in\mathbf{N} \mid x^2+2x+1=0\}?$$

- En général, pour montrer que $A=B$, il suffit d'établir que

  1. Pour chaque x, si $x\in A$ alors $x\in B$ et (ce qui montre $A\subseteq B$)
  2. Pour chaque x, si $x\in B$ alors $x\in A$ (ce qui montre $B\subseteq A$).

- Nous avons,

$$\mathbf{N}^*\subset\mathbf{N}\subset\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$$

- En général, pour montrer que $A\subset B$, il suffit de montrer la condition 1. et qu'il existe un élément de B qui n'est pas dans A.

- Est-ce que

$\sqrt{2}\in\mathbf{R}$?

Il faudrait définir **R** pour répondre formellement! Évidemment, la réponse est oui.

$\sqrt{2}\in\mathbf{Q}$?

Non!

L'ensemble puissance

- **Défn:** L'ensemble de tous les sous-ensembles (stricts ou pas) d'un ensemble A est appelé *l'ensemble puissance de* A, noté $\mathcal{P}(A)$.

$$\mathcal{P}(\{patate, carotte, robinet\}) = \{\varnothing, \{patate\}, \{carotte\}, \{robinet\}, \{patate, carotte\}, \{patate, robinet\}, \{carotte, robinet\}, \{patate, carotte, robinet\}\}.$$

$$|\mathcal{P}(\{patate, carotte, robinet\})| = 8.$$

- **Thm:** Soit A un ensemble de cardinalité finie. Alors,

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Opérations ensemblistes (I)

- **Défn:** Pour A et B deux ensembles, *l'union de* A et B, notée $A \cup B$, est l'ensemble $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$.
- **Défn:** Pour A et B deux ensembles, *l'intersection de* A et B, notée $A \cap B$, est l'ensemble $A \cap B = \{x \mid x \in A \text{ et } x \in B\}$.
- **Défn:** Pour A et B deux ensembles, *la différence entre* A et B (ou *complément de* A *relatif à* B), notée $A - B$, est l'ensemble $A - B = \{x \mid x \in A \text{ et } x \notin B\}$.
- Nous avons,

$$\mathbf{R} \cup \mathbf{Q} = \mathbf{R},\ \mathbf{N} \cup \mathbf{N}^* = \mathbf{N},\ \mathbf{R} \cap \mathbf{Q} = \mathbf{Q},\ \mathbf{N} - \mathbf{Q} = \varnothing,\ \mathbf{N} \cap \mathbf{N}^* = \mathbf{N}^*$$

- L'ensemble $\mathbf{R} - \mathbf{Q}$ est l'ensemble des nombres *irrationnels*.

Opérations ensemblistes (II)

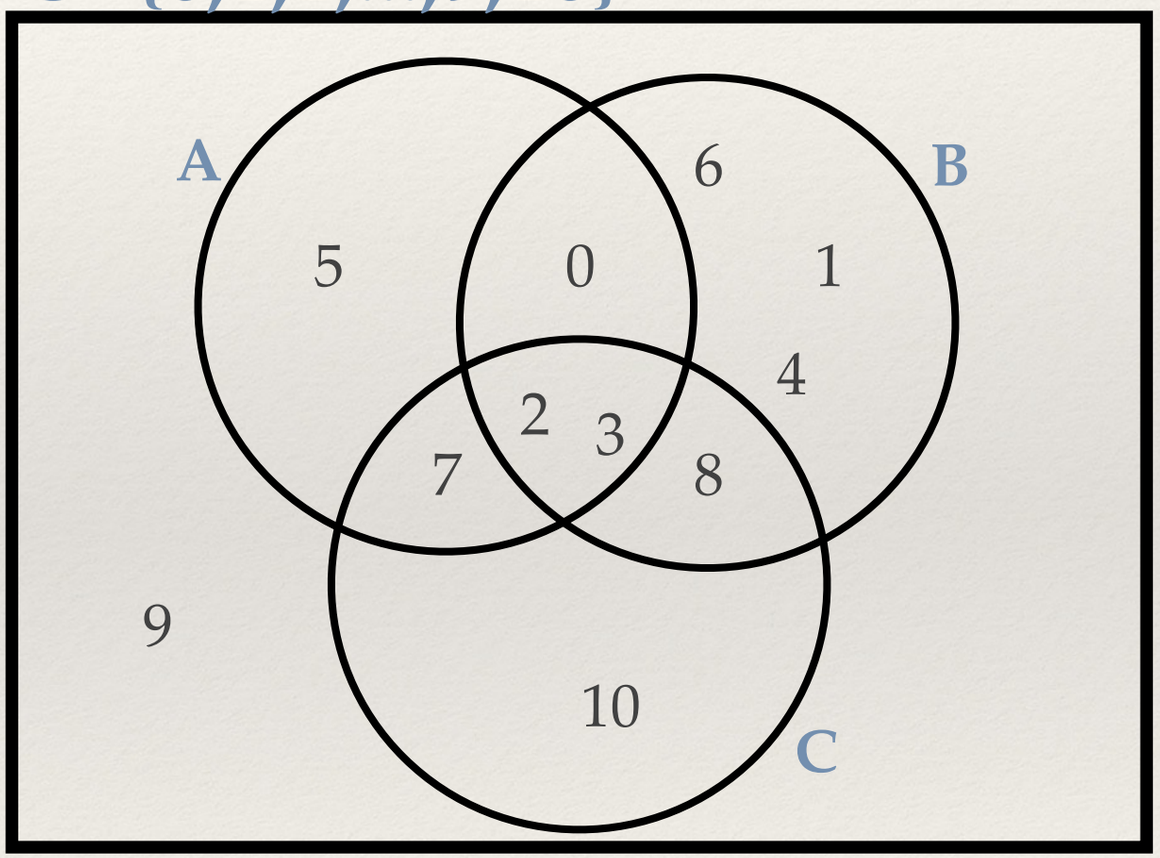
- **Défn:** Pour des ensembles A et B, si $A \cap B = \varnothing$ alors nous dirons de A et B qu'ils sont *disjoints*.
- **Défn:** Pour une collection d'ensembles C, nous dirons de C qu'elle est *disjointe en paire* si $A,B \in C$ tels que $A \neq B$ sont disjoints.

$C=\{\{1,2,5\},\{0\},\{3,4\}\}$ est disjoint en paire.

- **Défn:** Lorsque nous considérons des ensembles qui sont tous sous-ensembles d'un même ensemble U nous dirons que U est un *ensemble universel* ou un *univers*.
- **Défn:** Pour l'univers U et $A \subseteq U$, le *complément de* A, noté $\bar{A}$, est donné par $\bar{A}=U-A$.

Diagrammes de Venn

- Un diagramme de Venn est une représentation graphique des ensembles.
- L'univers est représenté par un rectangle et des ensembles de l'univers par des cercles à l'intérieur du rectangle de l'univers.
- L'intérieur d'un ensemble est représenté par l'intérieur du cercle qui le décrit. Deux ensembles qui ne sont pas disjoints seront représentés par deux cercles qui se recoupent.

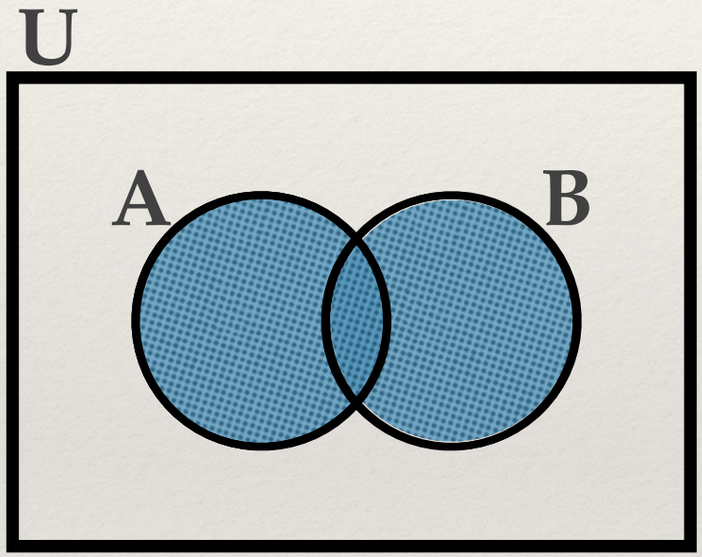


A={0,2,3,5,7}, B={0,1,2,3,4,6,8}, C={2,3,7,8,10}

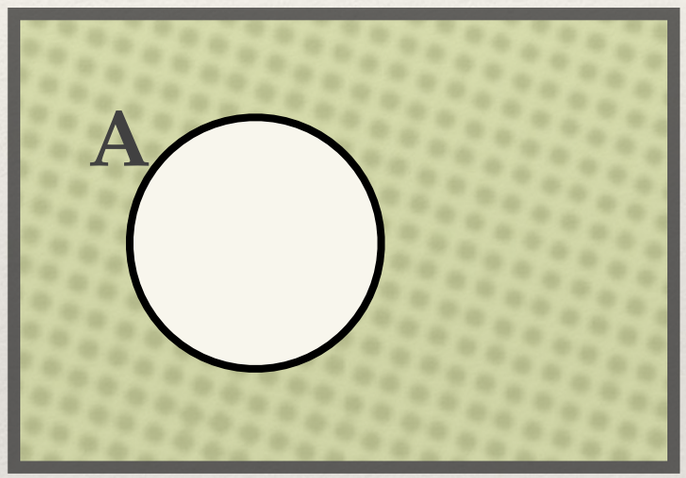
Vérification d'identités par diagrammes de Venn

- Vérifions l'identité suivante pour chaque paire d'ensembles A et B de l'univers U: $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$

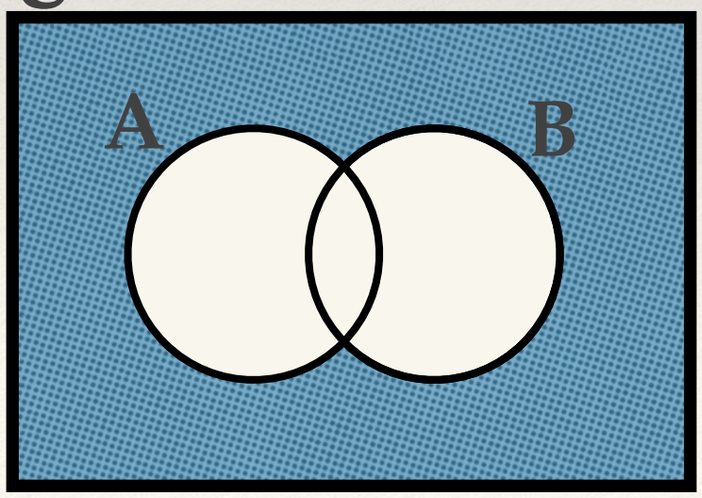
$A \cup B$



$\overline{A}$



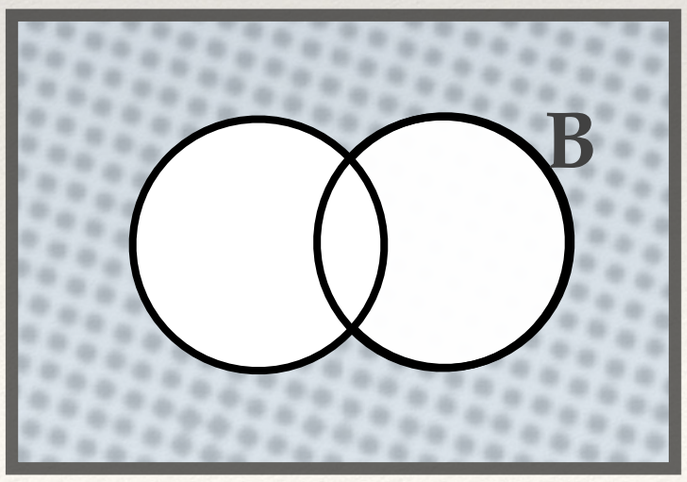
$\overline{(A \cup B)}$



Attention, ceci n'est pas une preuve formelle

$=$

$\overline{B}$



$\overline{A} \cap \overline{B}$

Propriétés utiles (I)

- Soit U un univers et soit A,B,C⊆U des ensembles sur un univers U. Nous avons,
  - Associativité de l'union et l'intersection:

$$(A \cup B) \cup C = A \cup (B \cup C) \text{ et } (A \cap B) \cap C = A \cap (B \cap C)$$

  - Commutativité de l'union et l'intersection:

$$A \cup B = B \cup A \text{ et } A \cap B = B \cap A$$

  - Distributivité:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ et } A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Propriétés utiles (II)

- Identités:

$$A \cup \varnothing = A \text{ et } A \cap U = A$$

- Complémentarité:

$$A \cup \overline{A} = U \text{ et } A \cap \overline{A} = \varnothing$$

- Idempotence:

$$A \cup A = A \text{ et } A \cap A = A$$

- Bornes:

$$A \cup U = U \text{ et } A \cap \varnothing = \varnothing$$

Propriétés utiles (III)

- Absorption:

$$A \cup (A \cap B) = A \text{ et } A \cap (A \cup B) = A$$

- Involution:

$$\overline{\overline{A}} = A$$

- Tout-ou-rien:

$$\overline{\varnothing} = U \text{ et } \overline{U} = \varnothing$$

- De Morgan (pour les ensembles):

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B} \text{ et } \overline{(A \cap B)} = \overline{A} \cup \overline{B}$$

Partitions (I)

- **Défn:** Pour S un ensemble d'ensemble (i.e. une famille d'ensemble). L'*union des éléments de* S, notée $\cup S$, est donnée par $\cup S=\{x \mid x\in X \text{ pour } X\in S\}$. L'intersection des éléments de S, notée $\cap S$, est donné par $\cap S=\{x \mid x\in X \text{ pour chaque } X\in S\}$.

- $S=\{\{0,2,5\},\{2,3,5\},\{0,2,4\},\{1,2,3\}\}$:
  - $\cup S=\{0,1,2,3,4,5\}$
  - $\cap S=\{2\}$
- $S=\{A_1,A_2,....\}$ avec $A_i=\{i,i+1,...\}$:
  - $\cup S=\mathbf{N}^*$
  - $\cap S=\emptyset$

Partitions (II)

- **Défn:** *Une partition d'un ensemble* A est un ensemble $\mathcal{P} \subseteq \mathcal{P}(A)$ tel que
  - $\cup \mathcal{P} = A$ et
    - pour chaque $X, Y \in \mathcal{P}$ avec $X \neq Y$, $X \cap Y = \emptyset$.
- {{1,4},{0,2,5}, {3,6}} est une partition de l'ensemble A={0,1,2,3,4,5,6}.
- Une partition $\mathcal{P}$ d'un ensemble A est donc une ensemble de sous-ensemble de A tel que chaque élément de A appartient à un seul ensemble de $\mathcal{P}$, c-a-d que $\mathcal{P}$ est *disjoint en paire*.

Paires ordonnées

- Tandis que les ensembles sont des collections d'éléments non-ordonnés, nous pouvons définir une collection d'objets pour laquelle l'ordre des éléments qu'elle contient est important. Un *vecteur* est de ce type.
- **Défn:** Une *paire ordonnée* des éléments a et b, notée (a,b), est distincte de la paire (c,d) à moins que $a=c$ et $b=d$.
- $\{(1,2),(3,3)\} \neq \{(2,1),(3,3)\}$ sont deux ensemble de paires ordonnées distinctes.

Produit cartésien

- **Défn:** Le *produit cartésien* entre les ensembles A et B, noté $A\times B$, est l'ensemble de toutes les paires ordonnées produites par un élément de A et un élément de B, $A\times B=\{(x,y)\mid x\in A \text{ et } y\in B\}$.

- $A=\{\text{patate, robinet}\}$, $B=\{0,1,2\}$

  $A\times B = \{(\text{patate}, 0),(\text{patate}, 1),(\text{patate}, 2),(\text{robinet}, 0),(\text{robinet},1),(\text{robinet},2)\}$

- Notons que $|A\times B|=|A|\cdot|B|$.

Attention,
$A_1\times A_2\times A_3 \neq (A_1\times A_2)\times A_3$

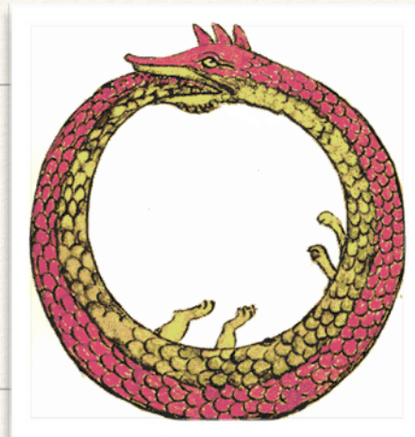
- $A\times B\neq B\times A$ lorsque $A\neq B$ avec A et B différents de l'ensemble vide.

- **Défn:** Le *produit cartésien entre les ensemble* $A_1,A_2,\ldots,A_n$, noté $A_1\times A_2\times\ldots\times A_n$, est donné par

$$A_1\times A_2\times\ldots\times A_n=\{(x_1,x_2,\ldots,x_n)\mid \text{ pour chaque } 1\leq i\leq n,\ x_i\in A_i\}.$$

- $|A_1\times A_2\times\ldots\times A_n|=|A_1|\cdot|A_2|\cdot\ldots\cdot|A_n|$.

Ensembles tordus



- Considérons l'ensemble
  - $A=\{x \mid x \in A\}$ définit à partir de lui-même. Il faut éviter de définir un ensemble de cette façon, même s'il s'agit d'une vérité. La définition d'un ensemble doit être unique et souvent les définitions auto-référentielles n'ont pas cette propriété. Par exemple:
    - $A=\{A\}$, est-ce que cet ensemble existe? Si oui alors est-il unique? (l'unicité est nécessaire)
- B=l'ensemble de tous les ensembles sur l'univers U.
  - $U=\{0,1\}$, $B=\{\varnothing, \{0\}, \{1\}, \{0,1\},\{\varnothing\}, \{\{0\}\}, \{\{1\}\}, \{\{0\},0\},...\}$
  - Est-ce que $B \in B$?
  - Utiliser un ensemble comme B mène souvent à des paradoxes. B n'est donc pas considéré comme un ensemble bien défini.

Paradoxe de Russell (et Zermelo)

- Considérons l'ensemble de tous les ensembles qui ne se contiennent pas eux-même. Est-ce que cet ensemble se contient lui-même?
  - Supposons que c'est le cas. Alors, cet ensemble se contient lui-même et ne peut donc pas être contenu dans l'ensemble des ensembles qui ne se contiennent pas eux-même, contredisant le fait que cet ensemble se contient lui-même.
- Supposons que cet ensemble ne se contient pas lui-même. S'il ne se contient pas lui-même alors il devrait être une ensemble de l'ensemble des ensembles qui ne se contiennent pas eux-même, contredisant le fait que cet ensemble ne se contient pas lui-même.
- On conclut que l'ensemble de tous les ensembles qui ne se contiennent ne peut ni se contenir lui-même ni ne pas se contenir lui-même. Un paradoxe!

Il ne s'agit pas d'un ensemble bien défini!

Une variante du paradoxe de Russell

- Sur une île perdue, un barbier coupe les cheveux de tous les insulaires que ne se coupent pas les cheveux eux-même.
- Est-ce que le barbier se coupe les cheveux lui-même?

- L'ensemble I des insulaires qui ne se coupent pas les cheveux eux-même est mal défini lorsque le barbier est inclus dans la population:
  - Le barbier se coupe les cheveux lui-même si et seulement s'il ne se coupe pas les cheveux lui-même!